REMARKS

The Examiner has rejected Claims 1-21 and 23-32 under 35 U.S.C. 103(a) as being unpatentable over Coss et al. (U.S. Patent No. 6,098,172) in view of Minear et al. (U.S. Patent No. 5,983,350). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to each of the independent claims.

With respect to each of the independent claims, the Examiner has relied on the combination of Coss and Minear to make a prior art showing of applicant's claim language. However, applicant notes that the Examiner has failed to apply specific citations from such references to all of applicant's claim language.

In particular, with respect to applicant's claimed technique "wherein the security policy is defined by a policy file which includes a policy file data structure stored as an XML (extensible markup language) document," the Examiner has failed to make a specific prior art showing of such claim language. After careful review of both the Coss and Minear references, applicant notes that neither reference teaches any sort of XML document, let alone with the specific contents claimed by applicant.

In addition, the Examiner has also failed to make a specific prior art showing of applicant's claimed technique "wherein a security policy section of the policy file data structure includes an entry for each security policy that is identified by a policy identifier field and is associated with a network protocol that is identified by a protocol identifier field." In fact, applicant notes that Coss teaches services (FTP, Mail, Telnet) being associated with each rule in a policy (see Figure 3 in Coss), but not that a "security policy... is associated with a network protocol that is identified by a protocol identifier field," as claimed by applicant (emphasis added). Furthermore, Minear also fails to teach such specific claim language.

Still yet, the Examiner has again failed to make a specific prior art showing of applicant's claimed technique "wherein at least one security policy is included for a TCP/IP network and includes a PPTP (point-to-point tunneling protocol), a RIP (routing information protocol), a

DHCP (dynamic host configuration protocol), an ARP (address resolution protocol), an Ident (identification protocol), ICMP (internet control message protocol) and VPN (virtual private networking) ports, and a NetBIOS (network basic input/output system) service." Applicant respectfully asserts that simply nowhere in either the Coss or Minear reference is there any teaching of at least one security policy being included for a "TCP/IP network and includes a PPTP...an ARP...an Ident...an ICMP...and VPN ports...and a NetBIOS...service" (emphasis added). Therefore, since neither reference teaches such specific protocols, ports and/or services, as claimed by applicant, it is clear that the Examiner's general reliance on the Coss and Minear references in rejecting such language is unfounded.

Yet again, the Examiner has failed to make a specific prior art showing of applicant's claimed technique "wherein a default setting for a high security policy on the TCP/IP network disallows incoming network traffic through the PPTP and ICMP ports, allows incoming network traffic through the RIP, DHCP, ARP and VPN ports, disallows access through the NetBIOS service to shared resources on the individual computer, and disallows the individual computer from using shared resources of other computers on the TCP/IP network, where incoming network traffic that attempts to access the individual computer using PPTP and NetBIOS is logged." Applicant respectfully asserts that neither the Coss nor Minear references teach any sort of "default setting for a high security policy," and especially not in the foregoing detailed setting claimed by applicant.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or

suggest all of the claim limitations, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has substantially incorporated the subject matter of Claim 23 into each of the independent claims along with the following claim language:

> "wherein the security policy associated with the network protocol is specific to the network protocol."

With respect to the subject matter of dependent Claim 23, presently incorporated into each of the independent claims, the Examiner has relied on the following excerpts from Coss and Minear to make a prior art showing of applicant's claimed technique "wherein the firewall configuration process is executed by the processing unit when the network address for the network adapter changes" (see the same or similar, but not identical language in each of the independent claims).

> "508: if a rule that applies to the packet calls for an address change, e.g., to a proxy or for insertion of one packet into another ("tunnel option"), the process returns to step 505 for processing based on the changed destination;" (Coss-Col. 7, lines 41-45)
>
> "8. A firewall, comprising:
>
> a first communications interface;
>
> a second communications interface;
>
> a first network protocol stack connected to the first communications interface, wherein the first network protocol stack includes an Internet Protocol (IP) layer and a transport layer;
>
> a second network protocol stack connected to the second communications interface, wherein the second network protocol stack includes an Internet Protocol (IP) layer and a transport layer;
>
> a security policy;
>
> a decryption procedure, operating at the IP layer of the first network protocol stack, the decryption procedure receiving encrypted messages received by said first communications interface and outputting decrypted messages; and
>
> an application layer proxy, connected to the transport layers of said first and second network protocol stacks, wherein the application layer proxy includes a plurality of authentication protocols, wherein each authentication protocol provides a different level of security, wherein

> the application layer proxy receives decrypted messages from the decryption procedure, selects an authentication protocol from the plurality of authentication protocols based on the content of the decrypted message, and executes the selected authentication protocol and wherein the application layer proxy determines based on the security policy whether the message is to be forwarded, and wherein the message is returned to the IP layer if the message is to be forwarded;
>
> a third communications interface; and
>
> a third network protocol stack connected to the third communications interface and to the application layer proxy, wherein the third network protocol stack includes an Internet Protocol (IP) layer and a transport layer and wherein the second and third network protocol stacks are restricted to first and second burbs, respectively." (Minear-Claim 8)

Applicant respectfully asserts that such excerpts do not meet applicant's specific claim language. In particular, neither excerpt teaches that "the firewall configuration process is executed...when the network address for the network adapter changes," as claimed by applicant (emphasis added). In fact, applicant notes that Coss even teaches *away from* applicant's specific claim language by disclosing a domain support engine that "determines which security policy to use for a new network session" (see Col. 6, lines 47-49-emphasis added). Thus, clearly applicant's claim language has not been met by either the Coss or Minear references.

With respect to applicant's presently claimed technique "wherein the security policy associated with the network protocol is specific to the network protocol," applicant respectfully asserts that neither the Coss nor Minear reference teach such claim language. In fact, Coss even teaches *away from* such claim language by disclosing a security policy table with a plurality of types of services (FTP, Telnet, Mail, etc.) associated with the rules of the policy (see Figure 3 and Col. 4, lines 17-19). In addition, Minear only teaches an IP layer of a network protocol stack (see Abstract). Thus, clearly neither the Coss nor Minear reference teach applicant's claimed network protocol-specific security policy.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. Just by way of example, with respect to dependent Claim 5 et al., the Examiner has relied on Col. 7, lines 61-67 in Coss along with Claim 8 in Minear to make a prior art showing of applicant's claimed technique "wherein the set of network addresses comprises at least one address outside the zone."

First, applicant respectfully asserts that Minear does not even suggest applicant's specific claim language, but instead only generally teaches a security policy. Second, Coss only teaches finding a table entry for which the IP address is present in the IP address range of the table entry. Clearly, the teaching of Coss does not meet applicant's specific claim language since Coss only discloses finding a specific table entry with a range of IP addresses for which the IP address is present, whereas applicant claims a zone defined by a set of network addresses (see Claim 3) where "the set of network addresses comprises at least one address outside of the zone" (emphasis added). Thus, applicant's claim language provides for zones being defined negatively by associating network addresses outside of the zone. In other words, the zone may be defined by network addresses that are not in the zone.

Again, since at least the third element of the *prima facie* case of obviousness has not been met, a notice of allowance or a proper prior art showing of all of the claim limitations, in the context of the remaining elements, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 41-43 below, which is added for full consideration:

> "wherein the network address dynamically assigned to the network adapter is determined by mapping an adapter registry identifier to an associated network address stored in an operating system registry" (see Claim 41);
>
> "wherein the network address dynamically assigned to the network adapter is determined by monitoring network traffic at the network adapter and examining a predefined limited amount of the network traffic to determine the network address" (see Claim 42); and
>
> "wherein the network address dynamically assigned to the network adapter is determined by receiving a network address from a network adapter device driver when the network adapter connects to the TCP/IP network" (see Claim 43).

Again, a notice of allowance or a proper prior art showing of all of the claim limitations, in the context of the remaining elements, is respectfully requested.

To this end, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

Reconsideration is respectfully requested.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. Applicants are enclosing a check to pay for the added claims. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P361/00.166.01).

Respectfully submitted,
Zilka-Kotab, PC

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100